

Chapitre 1- MENACES ET ATTAQUES

Hi, YOBOUE. When you submit this form, the owner will see your name and email address.

* Required

1

Concernant les protocoles de la couche transport, laquelle des affirmations suivantes est vraie ? (1 Point) 

- ☐ Le mode connecté du protocole TCP rend celui-ci invulnérable aux menaces de la couche transport.
- ☐ Le port côté client permet d'identifier l'application.
- ☒ Le protocole TCP assure la fiabilité de la session applicative.
- ☐ La non-fiabilité du protocole UDP est la source principale des menaces sur la couche transport.

2

Dans un environnement professionnel, pour cette photo, quel élément identifie une situation à risque (informations non protégées) ? * (1 Point)



Absence du propriétaire du bureau, accès à tous au bureau, session non verrouillé

3

Après avoir piraté des guichets automatiques à distance à l'aide d'un ordinateur portable, il a travaillé avec des fabricants de guichets automatiques pour résoudre les vulnérabilités. De quel type de hacker s'agit-il? * (1 Point)

- ☐ chapeau blanc
- ☒ chapeau gris
- ☐ chapeau noir
- ☐ chapeau bleu

4

Je visite des sites Internet pour mon plaisir, mais je crains de récupérer un code malveillant. Qu'est-ce qui sera le moins risqué ? (1 Point) 

- ☐ Télécharger des images
- ☐ Télécharger des logiciels de jeu
- ☐ Visualiser des films
- ☒ Recopier manuellement des textes

5

L'administrateur système du service informatique de mon entreprise me demande mon mot de passe au téléphone, pour faire des travaux de maintenance. Quelle est la meilleure attitude à adopter ? * (1 Point)

- ☐ Je vérifie qu'il s'agit bien de l'administrateur, je le lui donne et je le change juste après.
- ☒ Je ne le lui donne pas
- ☐ Je le lui donne, mais pas au téléphone, seulement de vive voix.
- ☐ Je le lui donne : l'administrateur a tous les droits. Lui refuser c'est prendre beaucoup de précautions pour pas grand chose.

6

Quelle est la vulnérabilité majeure de la couche transport ? (1 Point) 

- ☐ L'absence de chiffrement du contenu des paquets.
- ☐ L'absence d'authentification des en-têtes pour le protocole TCP.
- ☐ L'absence d'acquittement des paquets pour le protocole UDP.
- ☒ L'absence de contrôle d'accès sur les ports connus.

7

Son travail est d'identifier les faiblesses du système informatique de son entreprise. De quel type de hacker s'agit-il? * (1 Point)

- ☐ chapeau blanc
- ☐ chapeau gris
- ☐ chapeau noir
- ☒ chapeau bleu

8

Quelles actions font partie de celles menées lors d'une attaque par réinitialisation TCP ? (1 Point)

Please select 2 options.

- ☒ L'écoute active des communications TCP.
- ☐ La prédiction du numéro de séquence TCP.
- ☐ L'envoi d'un paquet TCP portant un flag FIN.
- ☒ L'envoi d'un paquet TCP portant un flag RST.

9

Lequel des éléments suivants est également considéré comme une attaque de commutateur (switch) ? (1 Point) 

- ☐ MAC spoofing
- ☐ DHCP spoofing
- ☐ Faux serveur DHCP
- ☒ ARP spoofing

10

un whaling est * (1 Point)

- ☒ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☐ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- ☐ un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☐ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☐ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable

11

Dans un environnement professionnel, pour cette photo, quel élément identifie une situation à risque (informations non protégées) ? * (1 Point)



Session non verrouillée en absence de la personne

12

un phishing est * (1 Point)

- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- ☒ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☐ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- ☐ un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☐ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☐ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable
- ☐ une technique d'attaque consistant à créer des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.

13

Quel est l'intrus? * (1 Point)

- ☐ bogue
- ☐ erreur de paramétrage
- ☐ erreur de fonctionnement d'un logiciel
- ☒ panne matérielle

14

Quelle propriété de sécurité est visée par une attaque par fragmentation ?
(1 Point) 

- ☐ Confidentialité
- ☐ Intégrité
- ☒ Disponibilité

15

Laquelle des attaques suivantes n'est pas une attaque DDoS ? (1 Point) 

- ☐ Inondation SYN
- ☐ Ping de la mort
- ☐ Attaque Smurf
- ☒ Man-in-the-middle

16

un SMiShing est * (1 Point)

- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☐ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- ☐ un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☐ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☐ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable
- ☐ une technique d'attaque consistant à créer des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.
- ☒ une utilisation des messages texte court sur des téléphones mobiles. Les criminels usurpent l'identité d'un contact légitime dans le but de gagner la confiance de la victime. Une attaque de ce type consiste, par exemple, à envoyer un lien de site web à la victime. Lorsque la victime consulte le site web en question, le malware est installé sur son téléphone mobile.

..

Que fait la commande suivante ? nmap -sP 192.168.0.0-100 (1 Point) 

- ☐ Balayage des ports
- ☒ analyse par ping
- ☐ analyse de vulnérabilités
- ☐ test d'intrusion

18

Dans un environnement professionnel, pour cette photo, quel élément identifie une situation à risque (informations non protégées) ? * (1 Point)



Noter le mot de passe

19

Je quitte mon poste de travail pour aller déjeuner. Je sais qu'il est recommandé de verrouiller ma session mais j'ai oublié de le faire et j'ai la paresse de revenir depuis le restaurant uniquement pour ça. Est-ce vraiment très imprudent ? (1 Point) 

- ☐ Oui, parce que l'ordinateur reste actif sous tension et consomme davantage d'électricité.
- ☐ Non, parce que l'ordinateur se verrouille automatiquement au bout d'un certain temps.
- ☐ Non, parce que si je ne suis pas là, je ne suis pas responsable de ce que ferait un visiteur.
- ☒ Oui, parce que n'importe qui aura accès à mes applications et données et en plus s'il fait quelque chose d'illégal, ma responsabilité peut être engagée.

20

L'exemple de Shoulder Surfing * (1 Point)

- ☐ prétendre être quelqu'un d'autre pour gagner la confiance d'une personne ou accéder aux zones ou données non autorisées.
- ☒ observer une victime pendant qu'elle saisit son code au distributeur automatique
- ☐ utiliser la tromperie pour provoquer la réaction irrationnelle d'un utilisateur
- ☐ suivre une personne autorisée pour accéder à un emplacement sécurisé ou une zone restreinte
- ☐ récupérer des documents dans une poubelle ou un conteneur de recyclage

21

un pharming est * (1 Point)

- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☒ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- ☐ un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☐ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☐ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable
- ☐ une technique d'attaque consistant à créer des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.

22

Citez une attaque contre le DHCP (1 Point)

Dhcp spoofing

23

Un ver est un * (1 Point)

- ☐ malware qui effectue des opérations nuisibles lors de l'ouverture d'une clé USB ou un disque
- ☐ programme malveillant qui utilise un déclencheur pour réactiver le code malveillant
- ☐ code malveillant utilisé pour compromettre un système à l'aide de portes dérobées.
- ☐ code malveillant exécutable à un autre fichier exécutable, comme un programme légitime
- ☒ code malveillant qui se reproduire en exploitant indépendamment des vulnérabilités dans les réseaux

24

Quel est le risque lié à un vol de cookie ? (1 Point) 

- ☒ Un attaquant peut récupérer le mot de passe de la victime.
- ☐ Un attaquant peut usurper l'identité de la victime auprès du site Web vulnérable.
- ☐ Un attaquant peut devenir administrateur du site Web.
- ☐ Un attaquant peut causer un déni de service au site Web vulnérable.

25

25

Quels sont les principaux paramètres qui sont ciblés par une attaque par inondation de paquets TCP SYN ? (1 Point)

Please select 2 options.

- ☒ Le nombre de sources de l'attaque.
- ☐ La longueur de la file d'attente des connexions semi-ouverte.
- ☐ Le temps de conservation d'une connexion dans la file d'attente des connexions semi-ouverte.
- ☒ Le débit des sources de l'attaque

26

L'exemple de Usurpation d'identité * (1 Point)

- ☒ prétendre être quelqu'un d'autre pour gagner la confiance d'une personne ou accéder aux zones ou données non autorisées.
- ☐ observer une victime pendant qu'elle saisit son code au distributeur automatique
- ☐ utiliser la tromperie pour provoquer la réaction irrationnelle d'un utilisateur
- ☐ suivre une personne autorisée pour accéder à un emplacement sécurisé ou une zone restreinte
- ☐ récupérer des documents dans une poubelle ou un conteneur de recyclage

27

Quels services de sécurité ne sont pas pris en charge par la cryptographie?

* (1 Point)

Enter your answer

28

Laquelle des attaques suivantes est une attaque DDoS réflexive ? (1 Point) 

- ☐ Ping of death
- ☒ Smurf
- ☐ Buffer overflow
- ☐ XSS

29

Identifier le type d'attaque qui utilise l'emprunt d'identité pour tirer parti d'une relation de confiance entre deux systèmes * (1 Point)

- ☐ Repérage
- ☐ Zero-day
- ☐ Man-In-The-Middle
- ☐ Keylogger
- ☐ DoS/DDoS
- ☒ Mystification

30

Concernant la pollution de cache DNS, lesquelles de ces affirmations sont vraies ? (1 Point)

Please select 2 options.

- ☒ La falsification de la section additionnelle d'une réponse DNS permet d'affecter des noms de domaine différents de la requête initiale.
- ☐ L'attaque requiert de "deviner" l'identifiant de la requête DNS.
- ☐ La pollution du cache DNS affecte uniquement les noms de domaine qui n'ont pas encore été mises en cache.
- ☒ La section additionnelle d'une réponse DNS peut comporter une fausse association entre une adresse IP arbitraire et un sous-domaine appartenant au même domaine que le sous-domaine inclus dans la requête.

31

Quel(s) dispositif(s) peut-on lier au service de confidentialité? * (1 Point)

- ☐ redondance
- ☒ chiffrement
- ☐ suppression des points de défaillance uniques
- ☐ sauvegardes des données

32

À quelle couche OSI l'usurpation d'adresse MAC se produit-elle ? (1 Point) 

- ☐ 1
- ☒ 2
- ☐ 3
- ☐ 4

33

Identifier le type d'attaque qui intercepte les communications entre les ordinateurs pour voler des informations pendant qu'elles transitent sur le réseau * (1 Point)

- ☐ Repérage
- ☐ Zero-day
- ☒ Man-In-The-Middle
- ☐ Keylogger
- ☐ DoS/DDoS
- ☐ Mystification

34

Laquelle des caractéristiques suivantes d'un commutateur malveillant pourrait lui permettre d'être la racine d'un arbre STP? (1 Point) 

- ☒ la plus adresse MAC
- ☐ la plus grande adresse IP
- ☐ un BPDU supérieur
- ☐ ID de routeur plus faible

35

Quelles sont les objectifs d'une attaque qui combine IP spoofing et amplification ? (2 réponses) (1 Point)

- ☒ atteindre une multitude d'hôtes grâce à une seule requête
- ☐ attaquer de manière indirecte une cible finale
- ☒ engendrer une réponse beaucoup plus volumétrique que la requête initiale
- ☐ utiliser le mécanisme IP fragmentation

36

Quelles entêtes un attaquant doit-il manipuler pour réaliser une attaque ICMP redirect ? (1 Point)

- ☐ Ethernet
- ☒ IP
- ☐ TCP
- ☒ ICMP

37

Il a travaillé avec des entreprises spécialisées dans la technologie pour résoudre un problème avec le DNS. De quel type de hacker s'agit-il? * (1 Point)

☒ chapeau blanc

☐ chapeau gris

☐ chapeau noir

☐ chapeau bleu

38

Le service informatique de mon entreprise m'a attribué un ordinateur portable pour mon travail c'est pratique. Quelle est la phrase fausse ? *
(1 Point)

☒ Je peux y mettre des données personnelles (photos, ...).

☐ Je peux l'apporter à la maison pour travailler dessus en local.

☐ Quand j'utilise Internet à la maison sur mon abonnement personnel, les outils de sécurité installés sur l'ordinateur me protègent aussi bien que lorsque je l'utilise au bureau.

☐ Je ne laisse personne d'autre que moi utiliser cet ordinateur.

39

Quel est l'intérêt principal pour un attaquant de forcer un switch à passer en mode hub ? (1 Point) 

- ☒ réaliser une attaque de déni de service tierce
- ☐ intercepter l'ensemble des communications des machines connectées sur ce switch
- ☐ éviter d'être identifiable
- ☐ usurper l'identité d'une autre machine

40

Lequel des éléments suivants pollue le contenu du cache DNS d'un ordinateur afin que les requêtes vers un site légitime soient acheminées vers un autre site ? (1 Point) 

- ☐ Phishing
- ☒ Pharming
- ☐ Vishing
- ☐ Whaling

41

Quelle est la meilleure solution à l'ingénierie sociale ? (1 Point) 

- ☒ sensibilisation
- ☐ listes d'accès
- ☐ Host-based IDS
- ☐ chiffrement

42

Un cheval de Troie est un * (1 Point)

- ☐ malware qui effectue des opérations nuisibles lors de l'ouverture d'une clé USB ou un disque
- ☐ programme malveillant qui utilise un déclencheur pour réactiver le code malveillant
- ☐ code malveillant utilisé pour compromettre un système à l'aide de portes dérobées.
- ☒ code malveillant exécutable à un autre fichier exécutable, comme un programme légitime
- ☐ code malveillant qui se reproduire en exploitant indépendamment des vulnérabilités dans les réseaux

43

Dans un environnement professionnel, pour cette photo, quel élément identifie une situation à risque (informations non protégées) ? * (1 Point)



Saisir le mot de mot sous les yeux attentifs de sa collègue

44

Un mail de ma banque m'avertit que mon compte a été débité de 80 mille Francs CFA par erreur. Pour me faire rembourser, je suis invité à cliquer sur le lien dans le message afin de confirmer mes coordonnées de compte.

Quel est le piège à éviter ? (1 Point) 

- ☒ Je clique sur le lien et je tombe sur le site de ma banque avec les cases à remplir. Je les remplis, c'est très simple.
- ☐ Je vais sur le site de ma banque en utilisant mes favoris dans mon navigateur pour voir ce qu'il en est.
- ☐ Je détruis le mail sans me soucier de la mise à jour de mes données bancaires.
- ☐ Je téléphone à ma banque et je traite cela par téléphone.

45

Trouver le service de sécurité portant sur le dispositif de protection par suppression des points de défaillance uniques. * (1 Point)

- ☐ Confidentialité
- ☐ anti-rejeu
- ☐ intégrité
- ☒ disponibilité
- ☐ contrôle d'accès

46

Pour vous, l'information sensible d'une entreprise, est-ce seulement ?
(1 Point) 

- ☐ L'information qui est connue uniquement de la Direction de cette entreprise
- ☐ L'information signalée par la Défense Nationale.
- ☒ L'information dont la divulgation peut mettre l'entreprise en difficulté.
- ☐ Ce qui touche au secret de fabrication.

47

Laquelle des attaques suivantes peut conduire à une attaque de type phishing ? (1 Point) 

- ☐ DHCP spoofing
- ☒ CAM overflow
- ☐ Double tagging
- ☐ Switch spoofing

48

un scareware est * (1 Point)

- une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour
- ☐ tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour
- ☐ tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☐ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de col-
- ☐ lecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☐ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☐ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable
- une technique d'attaque consistant à créer des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de
- ☒ l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.

49

Dans un environnement professionnel, pour cette photo, quel élément identifie une situation à risque (informations non protégées) ? * (1 Point)



Un document entier qui n'a pas été broyé

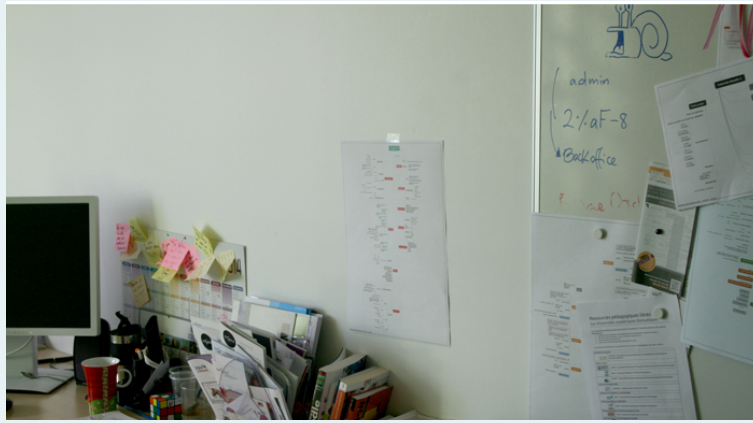
50

Laquelle des attaques suivantes est un exemple d'attaque de type VLAN hopping ? (1 Point) 

- ☐ Switch spoofing
- ☐ Man-in-the-middle
- ☒ LLDP reconnaissance
- ☐ ARP spoofing

51

Dans un environnement professionnel, pour cette photo, quel élément identifie une situation à risque (informations non protégées) ? * (1 Point)



Les accès sont écrits sur un papier collé sur le mur

52

Depuis son ordinateur, il a transféré 10 millions de francs FCFA sur son compte bancaire en utilisant les numéros de compte et les codes PIN de certaines personnes, après avoir visionné des enregistrements de ces personnes en train de saisir leurs numéros. De quel type de hacker s'agit-il?

* (1 Point)

- ☐ chapeau blanc
- ☐ chapeau gris
- ☒ chapeau noir
- ☐ chapeau bleu

53

L'exemple de piggybacking * (1 Point)

- ☐ prétendre être quelqu'un d'autre pour gagner la confiance d'une personne ou accéder aux zones ou données non autorisées.
- ☐ observer une victime pendant qu'elle saisit son code au distributeur automatique
- ☐ utiliser la tromperie pour provoquer la réaction irrationnelle d'un utilisateur
- ☒ suivre une personne autorisée pour accéder à un emplacement sécurisé ou une zone restreinte
- ☐ récupérer des documents dans une poubelle ou un conteneur de recyclage

54

Pourquoi un attaquant effectuant une attaque par inondation de messages echo request a tout intérêt à le faire en usurpant une adresse IP source ?
(1 Point)

- ☐ pour atteindre un plus grand nombre de victimes
- ☐ pour créer une attaque par amplification
- ☐ pour éviter d'être lui-même automatiquement attaqué, inondé par des messages
- ☐ car ICMP ne permet pas à une adresse source unique d'envoyer plusieurs messages echo request avec une fréquence trop élevée.

55

Un Ransomware est un * (1 Point)

- ☐ malware qui effectue des opérations nuisibles lors de l'ouverture d'une clé USB ou un disque
- ☐ programme malveillant qui utilise un déclencheur pour réactiver le code malveillant
- ☐ code malveillant utilisé pour compromettre un système à l'aide de portes dérobées.
- ☐ code malveillant exécutable à un autre fichier exécutable, comme un programme légitime
- ☐ code malveillant qui se reproduire en exploitant indépendamment des vulnérabilités dans les réseaux
- ☒ code malveillant retenant un système informatique (ou les données qu'il contient) captif jusqu'au paiement d'une somme d'argent.

56

Lequel des éléments suivants est généralement utilisé pour mettre en place une attaque de type "man-in-the-middle" ? (1 Point)

- ☐ ARP poisoning
- ☐ Dynamic ARP inspection
- ☐ faux switches
- ☐ MAC overflow

57

Quel type de hacker hacke pour une cause politique ? (1 Point)

- ☐ black hats
- ☐ white hats
- ☐ script kiddies
- ☐ hacktivists

58

Identifier le type d'attaque qui refuse l'accès aux utilisateurs autorisés, rendant inaccessibles le réseau, les services réseau ou les données sur le réseau * (1 Point)

- ☐ Repérage
- ☐ Zero-day
- ☐ Man-In-The-Middle
- ☐ Keylogger
- ☒ DoS/DDoS
- ☐ Mystification

59

Lequel des éléments suivants est une attaque de couche 2 du modèle OSI? (1 Point)

- ☐ Débordement de tampon
- ☐ DoS
- ☐ Empoisonnement à l'ARP
- ☐ Usurpation d'adresse IP

60

un spam est * (1 Point)

- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☐ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- ☐ un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☒ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☐ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable
- ☐ une technique d'attaque consistant à créer des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.

61

Laquelle des attaques suivantes fait fonctionner le switch comme un hub et non comme un switch ? (1 Point)

- ☐ Smurf attack
- ☐ CAM overflow
- ☐ SYN flood
- ☐ Fraggle attack

62

A quoi peut servir le mécanisme de ping (ICMP echo request, echo reply) pour un attaquant ? (1 Point)

Please select 3 options.

- ☐ à découvrir des machines accessibles et donc des victimes potentielles
- ☐ à usurper une adresse IP
- ☐ à effectuer une attaque de déni de service
- ☐ à ouvrir un port TCP sur une machine cible (pour ensuite s'y connecter)
- ☐ à fermer une connexion TCP existante
- ☐ à vérifier si une machine est vulnérable à une attaque ICMP redirect
- ☐ à découvrir partiellement la topologie d'un réseau

63

Quelle est la meilleure façon de ne pas se faire piéger par des gens qui vous « font parler » ? * (1 Point)

- ☐ Considérer tout son entourage comme suspect.
- ☐ Se méfier des gens qui vous proposent à boire.
- ☐ Bien identifier l'information sensible pour ne jamais en parler.
- ☐ Se méfier des gens qui vous proposent à boire.
- ☐ Éviter de se faire inviter au restaurant ou dans des soirées.

64

Un attaquant ayant le contrôle d'un domaine réseau peut détourner du trafic en abusant le protocole BGP. Quelles types d'annonce peut-il effectuer pour affecter le routage ? (1 Point)

Please select 2 options.

- ☐ Annoncer un chemin plus court.
- ☐ Annoncer un préfixe de destination locale.
- ☐ Annoncer un préfixe plus général.
- ☐ Annoncer un préfixe plus spécifique.

65

Laquelle des attaques suivantes inonde le commutateur avec des trames dont les adresses MAC source ne sont pas valides ? (1 Point)

- ☐ Smurf attack
- ☐ CAM overflow
- ☐ SYN flood
- ☐ Fraggle attack

66

un exemple de canular * (1 Point)

- ☐ prétendre être quelqu'un d'autre pour gagner la confiance d'une personne ou accéder aux zones ou données non autorisées.
- ☐ observer une victime pendant qu'elle saisit son code au distributeur automatique
- ☒ utiliser la tromperie pour provoquer la réaction irrationnelle d'un utilisateur
- ☐ suivre une personne autorisée pour accéder à un emplacement sécurisé ou une zone restreinte
- ☐ récupérer des documents dans une poubelle ou un conteneur de recyclage

67

L'utilisation du protocole ARP est-elle requise pour usurper une adresse MAC ? (1 Point)

- ☐ oui
- ☐ Non

68

Quel service de sécurité l'on recherche par l'application d'une fonction de hachage? (1 Point)

- ☐ intégrité
- ☐ confidentialité
- ☐ disponibilité
- ☐ non-répudiation

69

Un bombe logique est un * (1 Point)

- ☐ malware qui effectue des opérations nuisibles lors de l'ouverture d'une clé USB ou un disque
- ☒ programme malveillant qui utilise un déclencheur pour réactiver le code malveillant
- ☐ code malveillant utilisé pour compromettre un système à l'aide de portes dérobées.
- ☐ code malveillant exécutable à un autre fichier exécutable, comme un programme légitime
- ☐ code malveillant qui se reproduire en exploitant indépendamment des vulnérabilités dans les réseaux

70

Identifier le type d'attaque tentant d'exploiter des failles logicielles qui sont inconnues ou non divulguées par l'éditeur du logiciel. * (1 Point)

- ☐ Repérage
- ☒ Zero-day
- ☐ Man-In-The-Middle
- ☐ Keylogger
- ☐ DoS/DDoS
- ☐ Mystification

71

Un rootkit est un * (1 Point)

- ☐ malware qui effectue des opérations nuisibles lors de l'ouverture d'une clé USB ou un disque
- ☐ programme malveillant qui utilise un déclencheur pour réactiver le code malveillant
- ☒ code malveillant utilisé pour compromettre un système à l'aide de portes dérobées.
- ☐ code malveillant exécutable à un autre fichier exécutable, comme un programme légitime
- ☐ code malveillant qui se reproduire en exploitant indépendamment des vulnérabilités dans les réseaux

72

Vous exécutez une demi-connexion TCP et vous n'avez obtenu aucune réponse. Qu'est-ce que cela signifie? (1 Point)

- ☐ le port est ouvert
- ☐ le port est fermé
- ☐ le port est surveillé
- ☐ il ne peut pas être déterminé

73

Quelle est la raison pour un attaquant d'utiliser le mécanisme de "gratuitous arp" pour réaliser une attaque ARP poisoning ? (1 Point)

- ☐ usurper plusieurs adresses IP en une seule fois
- ☐ usurper une adresse IP de manière proactive
- ☐ forcer le switch à passer en mode hub

74

Lors d'une recherche pour trouver des exploits en matière de sécurité, il a rencontré une vulnérabilité de sécurité sur le réseau de l'entreprise auquel il est autorisé à accéder. De quel type de hacker s'agit-il? * (1 Point)

- ☒ chapeau blanc
- ☐ chapeau gris
- ☐ chapeau noir
- ☐ chapeau bleu

75

Quel est l'intrus * (1 Point)

- ☐ Erreur de configuration
- ☐ Pannes de matériels
- ☐ Dégâts des eaux
- ☐ Problème d'intégrité du bâtiment

76

L'exemple de Dumpster Diving * (1 Point)

- ☒ prétendre être quelqu'un d'autre pour gagner la confiance d'une personne ou accéder aux zones ou données non autorisées.
- ☐ observer une victime pendant qu'elle saisit son code au distributeur automatique
- ☐ utiliser la tromperie pour provoquer la réaction irrationnelle d'un utilisateur
- ☐ suivre une personne autorisée pour accéder à un emplacement sécurisé ou une zone restreinte
- ☐ récupérer des documents dans une poubelle ou un conteneur de recyclage

77

Quel est l'intrus? (1 Point)

- ☐ attaque par Force brute
- ☐ attaque par Dictionnaire
- ☐ Balayage des ports
- ☐ Ingénierie sociale

78

Supposons qu'un attaquant souhaite capturer l'ensemble du trafic réseau à destination d'une autre machine connectée au même sous réseau et au même switch que lui, quelles sont les solutions faisables ? (1 Point)

Please select 2 options.

- ☐ Envoyer des messages malformés à la victime
- ☐ Inonder le switch de messages avec différentes adresses Ethernet
- ☐ Utiliser l'adresse de diffusion en effectuant une attaque par inondation
- ☐ Réaliser l'attaque de VLAN hopping
- ☐ Utiliser l'ARP poisoning

79

un vishing est * (1 Point)

- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☐ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- ☐ un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☐ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☒ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable
- ☐ une technique d'attaque consistant à créer des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.

80

un spyware est * (1 Point)

- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification) des dirigeants d'une entreprise
- ☐ un code malveillant qui modifie les configurations des navigateurs
- ☐ une utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées (comme des informations d'identification), en se faisant passer pour une personne fiable.
- ☐ une utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en faisant passer ce site pour un site web fiable.
- ☒ un code malveillant transmis par e-mail ou téléchargé à partir de l'Internet, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes des navigateurs web ou des pages web
- ☐ un courrier indésirable utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs
- ☐ une utilisation des communications vocales pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable
- ☐ une technique d'attaque consistant à créer des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.



This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password.

Microsoft Forms | AI-Powered surveys, quizzes and polls [Create my own form](#)

